February 25, 1998

Director Freeh:

RE: SOLAR SUNRISE;
CITA MATTER
OO: HQ

The captioned investigation involves intrusions into computers within the United States which began around January 13, 1998, and continuing to date. The computers which have been compromised are computers belonging to the United States Air Force, located at Andrews AFB, Maryland, Kirkland AFB, New Mexico, Columbus AFB, Ohio, Lackland AFB, Texas, Gunter AFB, Alabama, and Channel Island, ANGS, California; computers belonging to the United States Navy, located at the United States Naval Academy in Annapolis, Maryland, Pearl Harbor, Hawaii, and computers belonging to the United States Marine Corps Base, Camp Butler, Okinawa, Japan.

Most of the compromised computers are Domain Name Servers (DNS), i.e. fbi.gov. DNS systems are responsible for translating domain names into their respective Internet Protocol(IP) addresses. IP addresses are essential for Internet computer communications. Intrusions into such computers have the potential to disrupt the mission of the U.S. military throughout the world.

From logs obtained from various Internet service providers and universities, investigators have determined that the intruder(s) originated from SONIC.NET an Internet service provider, in Santa Clara, California. Court Orders served on [redacted] revealed that [redacted]

b3
OTHER Sealed pursuant to court order

On February 9, 1998, the Massachusetts Institute of Technology (MIT) [redacted] contacted SONIC.NET regarding a computer intrusion. [redacted] at MIT, stated that someone had intruded their system from SONIC.NET and provided the Internet Protocol (IP) address. The IP address is known to be associated with [redacted] DOB [redacted]

b6
b7C

On February 16, 1998, electronic surveillance was initiated by the FBI on the user account [redacted] The Order was signed on [redacted]

b3
b6
b7C
OTHER Sealed Pursuant to court order

288-HQ-1242520-152

288-HQ-1242520

[redacted] b6 b7C
[redacted] are subjects of this investigation and are associates.

Another site identified as a "launching point" for the intrusions is Maroon.com, a web publisher located at College Station, Texas. [redacted] and a search warrant has been served for [redacted] b7E

A trap and trace Order was signed and executed on [redacted] A trap and trace Order is already in place for [redacted] b3

On [redacted] FBI SF initiated a Title III Order on [redacted] A Title III Order is now being pursued for [redacted] Additionally, [redacted] are also being obtain for each subject. b3 b7E

To date, 15 court orders have been served to include one Title III and two consensual monitoring sites. Two more orders are presently being obtained to include another Title III.

This matter is being coordinated with [redacted] DOJ, DOD, and others as new developments arise. Referral/Consult

K.M. Geide

NOT APPROPRIATE FOR DISSEMINATION TO THE PUBLIC

1 - [redacted]
1 -
1 -
1 -
1 -
1 -
1 -
1 -
APM:apm (11)

1 - Mr. Geide
1 - [redacted] b6 b7C
1 -

(03/31/95)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 2/24/1998

To: Director, FBI **Attn:** Acting Unit Chief [redacted]

From: WFO
C-17/NVRA
Contact: SSA [redacted] b6 b7C

Approved By: [redacted]

Drafted By: [redacted]:rar

File Number(s): 288-HQ-1242560 (Pending) -154

Title: SOLAR SUNRISE;
CITAC MATTERS;
OO: HQ

Synopsis: Following is the status of WFO's involvement in this investigation as of 2/24/98.

Reference: EC dated 2/17/98 to Houston Division.

Details:

288-WF-211047 "[redacted] U.S. NAVY - VICTIM; OO: WFO".

SA [redacted] is coordinating all investigative activity with Agents of the Naval Criminal Investigative Service (NCIS) based in both Washington, D.C. and Jacksonville, Florida. Trap & Trace/pen register installation still problematic. The subject's current whereabouts and employment are known. Coordination with the NCIS Agents will continue. Remote monitoring at [redacted] continuing. Intrusions through IAP.NET into MIT will be addressed by NCIS only. b3 b6 b7C

288-HQ-1242560 "SOLAR SUNRISE: CITAC MATTERS: OO: HQ"

Copies of [redacted] copied at FBIHQ CART were blank. Original evidence in the hands of [redacted] SSA [redacted] is following through to resolve. [redacted] related to the [redacted] account to be copied tomorrow by FBIHQ CART per CITAC. Access to account originated from the University of Phoenix, "online.uops.fo.uophx.edu." WFO will follow through.

b6 b7C b7E Referral/Consult